Task A - Activity 2 Template: Cyber security plan for the networked system

Protection Measure 1:

1) **Threat(s) addressed by the protection measure**: 1 and 4, Attack Via Internet Connection and Misconfigured/unsafe firewall

Size of Loss: Major

2) **Details of action(s) to be taken:**
Configure a complex password policy, for users logging in to network and accessing secure areas of the network.

Install or activate a firewall on the router.

Secure all ports on the network.

Configure MAC filtering, so that only devices with a certain MAC address within the company or outside can access the network.

Check and configure the firewall to allow access to network through VPN, only if it is being accessed through a certain port/ports and block entry to the network through open ports.

3) **Reasons for the actions**
Ensuring that all users use complex password, will better protect the network, and ensure that passwords cannot be guessed by password generating software and attackers. This will make it harder for attackers to gain access to the network and lower the chance of this.

Attacks can be successful if a network is using common known and default ports. Changing the ports to different numbers will make it harder to gain unauthorised access to the network. If the ports are open and unsecured, it will make it easier for an attacker to gain access to the network.

Firewalls protects the network and increases the security of it. It protects the network from unauthorised access. The firewall will block attempts to gain access to the network unless a user enters through the correct port. This is useful for clients and staff when accessing the network through the VPN at home, work or at client locations.

If MAC filtering is used, it would allow for authorised devices to connect to the network. This would mean if a device attempts to access the network and it is not on the MAC filter list of approved devices, it will not be able to gain access to the network. This can be used so that only certain devices from clients and staff can access the network.

Firewalls protect the network. The firewall will block access to the

network, until a user has entered the correct port number, to gain access to the network.

4) **Overview of constraints – technical and financial**

Technical

Minimal, setting up and configuring a firewall is easy, especially if Baljinder has the relevant knowledge. Instruction manual will guide the user too, in order to set this up.

Financial

Minimal, depending on the router currently in place within BCTAA. Nearly all modern routers have firewalls built into them. If the router does not have a firewall built in, it will come at a cost.

5) **Overview of legal responsibilities**

Legal Responsibilities

Ensuring that confidential information is securely kept and not shared with anyone apart from authorised people. Also need to ensure that the data is protected and complying with data protection act.

6) **Overview of usability of the system**

Usability

Minimal, however, if MAC filtering is configured and a user's device is incorrectly blacklisted, they will not be able to gain access to the network, until that device is added to the whitelist of approved devices, which may take time to do.

If passwords are required to be complex, this may cause logging in issues as users may forget their passwords or block their account, with too many login attempts.

7) **Outline cost-benefit**

This may come at no cost, especially if the router already in place has a firewall built in. Modern routers have MAC filtering and firewalls built in. All that is needed is configuration and the enforcement of complex passwords. The benefits of this would mean that attacks to the network are likely to fail and data cannot be lost and accessed by unauthorised people.

8) **Test plan**

Test plan

Test No	Test description	Expected outcome	Possible further action following test
1	Entering a password which doesn't mean the "complex	A user should not be allowed to login with this password,	If the password is allowed to be set to a non-complex password, the

	password" criteria of capitals, symbols and numbers.	or be able to change their password to a non-complex password.	network/server security policy should be changed to allow only complex passwords.
2	Login to network from device outside of the company, via a VPN.	Network login should fail. Unless the device being accessed, its MAC address is on the MAC filtering whitelist.	Re configure/add devices to MAC whitelist and blacklist
3	Check all ports on the firewalls	This should show all open and unsecured ports on the network and firewall.	If ports are open and unsecured, close them or secure them, so the network cannot be accessed through these. Only use required ports.

Protection Measure 2:

1) **Threat(s) addressed by the protection measure**: 2, 7, 9, 12
Network access by mobile devices from staff and visitors, Insufficient user rights, resulting in unauthorised access, Misconfigured Wi-Fi, Staff and guests having access to the same network.

Size of Loss: Major

2) **Details of action(s) to be taken:**

Create/Install separate Wireless Access Points for staff, (including freelance trainers and assessors) and a Wireless Access Point for client visitors.

Configure MAC Address filtering to only allow mobile devices to access the network who are on the whitelist.

Using complex passwords on wireless access points.

Configure different access rights, for different user groups.

3) **Reasons for the actions**
The creation of different Wireless Access Points for staff and client visitors, allows different user groups to connect to the network and access it. This way it allows for visitors to only access appropriate areas of the network and not gain access to staff areas, and staff to only access areas of the

network that are relevant to staff.

Using a MAC address filtering solution, with whitelists, would only allow for authorised devices to gain access to the network. Any device not on the whitelist will be blocked from accessing the network.

The use of complex passwords on Wireless Access Points, makes it harder to gain access to a network.

Access rights can be configured to ensure that staff have different access rights to the network compared to client visitors. This way staff can access appropriate areas of the network when they have to and client visitors can only access appropriate areas of the network and not view other secure areas. This way data security is protected and cannot be compromised.

4) **Overview of constraints – technical and financial**

Technical

Minimal, setting up and configuring separate wireless access points would be easy, as if Baljinder is experienced and has the knowledge to do this, it would be achievable. Instruction manuals can also act as a guide.

Adding devices to the whitelist, involves having access to the device that needs to be added to the whitelist, and entering its MAC address into the whitelist, which is simple to do and set up. It would also be time consuming to frequently update, add and delete devices from the whitelist. Some routers limit the number of devices that can be on a whitelist, to 25 addresses, which means only 25 staff devices can access the network, as well as 25 client visitors. This may not be enough and may require a new router or new access point to be created.

Minimal, access rights can be configured easily and requires little set up.

Financial

Minimal, most modern routers, allow for separate wireless access points to be created. Most business routers and wireless access points also have MAC filtering functionality including whitelists and blacklists built in. There will be a cost, if these are not available in the current router.

5) **Overview of legal responsibilities**

Data on each wireless access point and secure areas will need to be protected.

6) **Overview of usability of the system**

Usability, should improve, if MAC filtering is used correctly. Only authorised devices can access the network.

If passwords are required to be complex, this may initially cause logging in issues as users may forget their passwords or block their account, with too many login attempts. Wrong passwords for wireless access points, means devices won't be able to connect to the network.

7) **Outline cost-benefit**
If network access was compromised and data was lost, this would have a profound impact on BCTAA's reputation and image. The impact of this would be catastrophic for the company, therefore it is important that these actions are put in place and applied. The different wireless access points should be configured and set up, so that staff and visitors can only access secure appropriate areas each. MAC filtering should also be implemented too, however if there are lots of staff and visitors, the wireless access points may not be able to add all these devices to the whitelist, which is a disadvantage of MAC filtering. It is also time consuming and would have to be updated regularly.

8) **Test plan**

Test plan

Test No	Test description	Expected outcome	Possible further action following test
4	Log in onto client visitors wireless access point	Client visitor should only be allowed to view the appropriate client secure area, if they successfully enter the correct login credentials. It should not contain trade secrets of other clients, and should also not have access to other areas of the network such as staff.	Use latest password technology for wireless access point to make it as secure as possible, such as WPA2, to encrypt data.
5	Log in onto client visitors wireless access point	Staff should only be allowed to view the appropriate staff secure areas, if they successfully enter the correct login credentials. It should not contain trade secrets of other clients, and should also not have access to other areas of the network such as staff.	Use latest password technology for wireless access point to make it as secure as possible, such as WPA2, to encrypt data.
6	Login with different user types.	Depending on the credentials entered, it should log the user into the staff area, or client visitor area.	Configure access rights further, so that staff access staff areas only and client visitors only access appropriate areas.

Protection Measure 3:

1) **Threat(s) addressed by the protection measure**: 3, Attack/theft of client information

Size of Loss: Major

2) **Details of action(s) to be taken:**
Encrypt data and files that are stored on the network, client information is stored within secure areas of the network.

Configure access rights/user groups so that to only authorised people can view, delete, update and edit files.

3) **Reasons for the actions**
Files on the network have to be protected and encrypted. This is because they contain trade secrets of clients as well as highly confidential information, and if this information was stolen by attackers, they could share this data with other people who could use it to bring down the client/client's company, which would not be good.

If files are encrypted, it would be hard for attackers to decrypt the files and gain access to them, as they would need the encryption key, which is randomly generated and cannot be found out by software.

If user rights are configured, it would be hard for attackers to gain access to different areas, as they would have to guess login credentials correctly. If an attacker gained access to an account with lower access rights, it would be harder for them to steal data from the network as well attacking it.

4) **Overview of constraints – technical and financial**
client information is stored within secure areas of the network.
Technical
Minimal, encryption is easy to setup and configure on the network, so that files and data is constantly protected. Access rights and user groups are also easy to configure and set up. Instruction manuals and Baljinder's knowledge could come to use.

Financial
Minimal, encryption of data and files costs nothing, as it is built into all modern computers and computer networks, running the latest operating systems. The same applies to access rights.

5) **Overview of legal responsibilities**
Maximal/Important. As BCTAA is handling confidential client data, it will need to ensure this data is protected and secure, otherwise it can face legal implications for failing to comply with the data protection act.

6) **Overview of usability of the system**
Usability
Minimal, Access rights/user groups and encryption of files and data on the network would only have to be set up once. The operating system would automatically do this when this has been set within the settings panel.

7) **Outline cost-benefit**
There is a minimal cost involved, therefore these changes should be listened to and put into place. If there was to be an attack on the network and BCTAA's unencrypted files were stolen, BCTAA could face legal and financial implications for failing to protect the data of its clients. It is therefore imperative that these measures are put in place.

8) **Test plan**

Test plan

Test No	Test description	Expected outcome	Possible further action following test
7	Login as client visitor and attempt to access staff area and files.	The client visitor should not be allowed to view this area on the network or access it.	Login as a client visitor and try to view client area, and access should be granted. Login as staff and try to view client and staff area, and access should be granted. If not, re-configure access rights.

Protection Measure 4:

1) **Threat(s) addressed by the protection measure**: 5, 8
Unauthorised use of ports, Physical Access to 19th floor

Size of Loss: Moderate

2) **Details of action(s) to be taken:**
Install protective RJ45 port blockers to each port, if not in use.
Collect and analyse entries into the data outlet rooms.

3) **Reasons for the actions**
Unprotected RJ45 ports, means people can connect their devices to them and gain access to the network. This can allow unauthorised people and

attackers to enter the building, connect their devices secretly and steal data from the network in the process, with hacking devices. Port blockers would also protect the ports from dust and from wear and tear damage that may occur over time and during the transport of devices.

The data outlet rooms contain the server and other important components of the BCTAA network. Collecting and analysing staff and visitors who enter into the data outlet rooms will allow for the company to spot unusual behaviour and stop potential employee sabotage as well as visitor sabotage.

4) **Overview of constraints – technical and financial**

Technical

Minimal, installing port blockers to ports and on devices such as computers require minimal technical knowledge and ability.

Analysing entries may involve reviewing CCTV footage or card entry statistics.

Financial

Minimal, although, port blockers do come at a cost. However, this is cheap and if bought in bulk, can be even cheaper. The port blockers will help to limit unauthorised physical connections to the network from hackers and help to reduce wear and tear of the ports. If the card reader system provides information about statistics and employees who enter the room, then cost is minimal, otherwise it may come at an expense to install CCTV cameras.

5) **Overview of legal responsibilities**

If data is secured and protected, then BCTAA are complying with legal responsibilities such as data protection act and computer misuse act.

6) **Overview of usability of the system**

Minimal, although if access is needed to the port, or they need to connect their devices through the port, they will have to get the port blocker out of the ports.

7) **Outline cost-benefit**

The minimal costs associated with buying the port blockers are a positive advantage. It is cheaper to protect the ports, and they provide a greater sense of security. It is imperative that this is done. CCTV cameras being installed may be expensive, however the benefit of this is that it allows for company to spot potential sabotage.

8) **Test plan**

Test plan

Test No	Test description	Expected outcome	Possible further action following test
8	Install port blocker onto unused data outlet patch panel	When attempting to remove the port blocker, it should not budge and should only be able to be removed with the port blocker removal key.	If the port blocker is easily removable without the key, a more expensive port blocker should be considered, to limit physical, unauthorised access to the network.
9	Install port blocker onto unused ports on devices.	When attempting to remove the port blocker, it should not budge and should only be able to be removed with the port blocker removal key.	If the port blocker is easily removable without the key, a more expensive port blocker should be considered, to limit physical, unauthorised access to the network.

Protection Measure 5:

1) **Threat(s) addressed by the protection measure**: 6, Access to network away from premises/Misconfigured NAT

Size of Loss: Major

2) **Details of action(s) to be taken:**
Turn on NAT and configure it so it is not on default settings.

3) **Reasons for the actions**
If the NAT is not configured correctly or turned on, it would prevent staff and client visitors from being able to access the network away from the premises such as at client locations. This would mean the staff are unable to do their job. If the NAT was not configured properly, this would create a vulnerability in the network, which can be exploited and infiltrated by attackers who can access the network.

4) **Overview of constraints – technical and financial**
Technical
Minimal, set up and configuration is easy due to instruction manuals and tutorials available.

Financial
Minimal, NAT settings and functionality are built in routers. If it is not available in the current router, purchasing a new router would come at a cost for BCTAA. The best VPN's come at a cost.

5) **Overview of legal responsibilities**

Must ensure data is protected even remotely.

6) **Overview of usability of the system**

Minimal, it would now be easy for staff and client visitors to access the BCTAA network, when they are outside of its premises at home and at client locations through VPN software which would facilitate this.

7) **Outline cost-benefit**
Enabling NAT will allow for staff to conduct their work away from the BCTAA premises. VPN's come at a cost unfortunately. However, it is a requirement that staff and client visitors can gain access to the network remotely outside the premises through a VPN. Therefore, this must be implemented, no questions asked.

8) **Test plan**

Test plan

Test No	Test description	Expected outcome	Possible further action following test
10	Attempt to login as a staff member remotely, away from BCTAA premises, via a VPN.	The connection should be successful, and the staff should be able to access the network and secure areas.	If the login is not successful and the staff member cannot login or view areas, NAT would need to be re-configured correctly.

Protection Measure 6:

1) **Threat(s) addressed by the protection measure**: 10, Lack of Network Specialist

Size of Loss: Moderate

2) **Details of action(s) to be taken:**
Configure the network so that it is easier to use and access

Communicate with and inform Baljinder Singh that the company needs a network specialist/he needs network training to improve his skills.

3) **Reasons for the actions**
The network must be easy to use, so that in the event of technicians or IT support workers available, someone within the company can help get the network back up and running, so it doesn't impact upon BCTAA's productivity. Adding shortcuts to network pages, would make the network easier to use, as well as adding help guides and tutorials in secure areas

of the network, in the event of network failure and there is no specialist available.

The BCTAA Network needs a network specialist. This is because a network specialist would be in charge of monitoring, maintaining, updating and running of the server and network. At the moment, the scenario says that the current system "had stuff added when we thought it was needed". If there is no network specialist, in the event of the system going down, no one would be able to get it back up and running again, especially if there are no specialists.

4) **Overview of constraints – technical and financial**

Technical

Minimal, set up and configuration of the network to be more friendly is easy due to instruction manuals and tutorials available.

Financial

Minimal, to configure the network to be easier to use, comes at no cost, if the operating system is up to date. However, if Baljinder Singh decided to listen and upskill his current skills towards a network specialist, these course and network specialist training sessions cost money, and the best qualifications can be very expensive. Alternatively, hiring someone to fill in this role, would also be expensive.

5) **Overview of legal responsibilities**

If data is secured and protected, then BCTAA are complying with legal responsibilities such as data protection act and computer misuse act.

6) **Overview of usability of the system**

Minimal, configuring the network to be even easier to use, would make it more usable and user friendly, for staff and visitors to access the network. Ensuring that a network specialist is available, would increase usability of the system, as they specialist would be able to use their knowledge and skills to configure the system to better suit the needs of the company and make it more efficient.

7) **Outline cost-benefit**

There is a benefit in ensuring that a network specialist is available. That benefit is that they will be able to run and maintain the system to ensure it is protected and secured. However, this comes at a cost. A specialist must be hired to fill in this role, or Baljinder must undertake some form of training, in order to gain the skills and knowledge required for the role. The scenario says Baljinder is responsible for the current network, but he is not a qualified network specialist. It is better that a network specialist is put in place, to ensure that the network is as secure and protected as much as possible.

8) **Test plan**

Test plan

Test No	Test description	Expected outcome	Possible further action following test
11	Attempt to test Baljinder's network skills in terms of running and maintaining the network.	Baljinder should either be able to run the network successfully and have the required skills, or he is not at the required skills level, in order to maintain the network to a high standard as possible.	Make Baljinder undertake some form of training

Protection Measure 7:

1) **Threat(s) addressed by the protection measure**: 11, Un-organisation of Network addresses

Size of Loss: Major

2) **Details of action(s) to be taken:**
Allocate static or dynamic addresses to each device on the network

3) **Reasons for the actions**
If the Network address are unorganised, it could leave the network more vulnerable to hacking attempts. If an attack was successfully launched, attackers could gain access to the network. Assigning static addresses to devices means that the address of a device will not change when the device is turned off and then turned on at a later stage.

4) **Overview of constraints – technical and financial**
Technical
Minimal, set up and configuration of static and dynamic addresses is simple to do, due to there being instruction manuals widely available.

Financial
Minimal, nearly all routers allow for devices to be assigned static or dynamic addresses if configured correctly. All the latest operating systems allow for this to occur too. If the router or operating system is too old and doesn't have this functionality, it would come at a cost.

5) **Overview of legal responsibilities**

If data is secured and protected, then BCTAA are complying with legal responsibilities such as data protection act and computer misuse act.

6) **Overview of usability of the system**
The assignment of static addresses would make the network more usable, as the network should allow the device to connect, as the address is the same and doesn't change, which could potentially cause login and network accessing problems.

7) **Outline cost-benefit**
Enabling static addresses will allow for staff and client visitors devices to have the same, fixed address, no matter if they reset, reboot or turn on and off their device. It comes at very little cost, especially if the router and operating system is up to date. This must be implemented.

8) **Test plan**

Test plan

Test No	Test description	Expected outcome	Possible further action following test
12	Use a staff member device and repeatedly reboot and reset the device.	The network address should be static and should remain the same no matter what.	Consider changing some devices to use dynamic address.
13			

Protection Measure 8:
1) **Threat(s) addressed by the protection measure**: 13, BCTAA server appearing on the Wi-Fi network

Size of Loss: Moderate

2) **Details of action(s) to be taken:**
Configure server settings and set server as hidden and not broadcasting.

3) **Reasons for the actions**
Hiding the server from view, means people won't know that it exists. Hiding it means that attacks are less likely to happen, because they don't know there is a server which has information. If the server displayed, they would want to gain access to try and access the files.

4) **Overview of constraints – technical and financial**

Technical
Knowledge is required, as it involves using Registry Editors and Command prompt.

Financial
Minimal, as Registry Editors and Command Prompts are part of the operating systems of the computers on the network.

5) **Overview of legal responsibilities**
Must ensure data is protected.

6) **Overview of usability of the system**
May make it harder to access the server, as the IP address of the server will have to be known. To make it more usable, shortcuts could be created on computers.

7) **Outline cost-benefit**
There is no cost to this, so this should be implemented to protect the network.

8) **Test plan**

Test plan

Test No	Test description	Expected outcome	Possible further action following test
14	Edit the server settings through Registry Editor and Command Prompt.	The server should now disappear from the network and be hidden.	If server displays on the network, reconfigure or alternatively look at guides.